USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: 6/3/2022

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

OPTIONALITY CONSULTING PTE. LTD,

Plaintiff,

-against-

EDGE TECHNOLOGY GROUP LLC et al.,

Defendants.

----------X

18-CV-5393 (ALC) (KHP)

OPINION AND ORDER

KATHARINE H. PARKER, United States Magistrate Judge:

Before this Court are three discovery-related motions. As they are substantially related, the Court addresses them together below. Specifically: (i) Defendants have moved for a protective order requiring identification of trade secrets and confidential information (ECF No. 82); (ii) Plaintiff has cross-moved to compel the production of documents and information (ECF No. 86); and (iii) the parties jointly move to seal Exhibit B to Plaintiff's memorandum of law in support of its motion to compel (ECF No. 85). For the reasons set forth below, Defendants' motion is DENIED, Plaintiff's cross-motion is GRANTED in part and DENIED in part, and the joint motion to seal is GRANTED.

BACKGROUND

The Court assumes familiarity with the facts and thus does not elaborate on the factual assertions except as needed for context.[1] In short, Defendants claim to be at a loss in determining what if any trade secrets or confidential information of Plaintiff they possess, and thus must produce. In its amended complaint, Plaintiff alleges that the relevant

[1] For a full recitation of the facts see *Optionality Consulting PTE. LTD. v. Edge Tech. Grp. LLC*, 2021 WL 310942, (S.D.N.Y. Jan. 29, 2021).

misappropriated information includes "tools, formulas, templates, information about specific project opportunities, business strategy and plans, the related technical and non-technical information, discoveries, improvements, processes, formulae, data, inventions, materials, and other information that is useful or necessary to this program[.]" (ECF No. 33 ¶ 140).

Since the beginning of discovery, Defendants have produced approximately 4,000 pages of documents to Plaintiff including all communications between the parties and all documents relating to CyberSAIF. (Def. Mot., ECF No. 82.) During the instant briefing, Plaintiff provided Defendants over a thousand documents to aid Defendants in determining what trade secrets and confidential information of Plaintiff they may possess. Defendants retort that these documents, which include e-mails it produced and pitch materials, do not provide them with the necessary particularity to comply with Plaintiff's discovery requests. Plaintiff avers that the particularity provided at this stage of the litigation is sufficient to obtain the requested discovery and no further clarity is warranted.

In letters exchanged between counsel to attempt to resolve the issue, Plaintiffs noted that its confidential information includes the specific protocol for running the internal penetration test in a way that will meet industry and regulatory-specific standards and yield actionable results. (ECF No 87, Exs. I-J.) Plaintiff also asserted that in addition to developing the framework, policies, and procedures for CyberSAIF, it created "comprehensive tools, formulas, templates, processes, and reports necessary to (1) yield the appropriate IT data harvest; (2) process such information; and (3) turn such information into a CEO-level readable,

actionable 'Risk Assessment Report' necessary to assist hedge funds in meeting their cybersecurity needs." ECF No. 87; *see also* ECF No. 33 ¶ 24.

Defendants have also objected to eight of Plaintiff's documents requests. Specifically, Defendants object to the following requests:

> 19. All documents and communications related to your formal or informal plans, drafts, proposals or Statements of Work for any cybersecurity service offered by you;
> 23. All documents and communications related to [Edge employee Tommy Mazzola's] work on and responsibilities in relation to any cybersecurity offering;
> 31. All documents and communications related to the GPDR [the EU General Data Protection Regulation] including but not limited to documents and communications related to any privacy services you offered, contemplated offering or currently offer;
> 38. All Statements of Work prepared by you for any current, former, or potential client from January 1, 2016 to present;
> 45. All documents you prepared for or provided to any of your current, former, or potential clients related to the advertising, sale, promotion, or marketing of cybersecurity services from March 2017 to the present date;
> 48. An accounting of your revenues and profits from the sale of your cybersecurity products, with the exception of CyberSAIF, to any third person;
> 49. An accounting of your total revenues and profits;
> 50 An accounting of your total sales.

(Defs. Opp. to Mot. to Compel, ECF No. 88.)

DISCUSSION

1. **Applicable Legal Standard**

A district court has "wide latitude to determine the scope of discovery," and "abuses its discretion only when the discovery is so limited as to affect a party's substantial rights." *In re Agent Orange Prod. Liability Litig.*, 517 F.3d 76, 103 (2d Cir. 2008) (citation omitted). The Federal Rules provide that:

> Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.

Fed. R. Civ. P. 26(b)(1). In making rulings on the scope of discovery, a court "must limit the frequency or extent of discovery otherwise allowed by these rules" if:

> (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;
> (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
> (iii) the proposed discovery is outside the scope permitted by Rule 26(b)(1).

Fed. R. Civ. P. 26(b)(2)(C). Lastly, Fed. R. Civ. P. 1 provides that the Rules be "construed and administered to secure the just, speedy, and inexpensive determination of every action and proceeding."

When carrying out its duty to manage litigation, a court "may, for good cause issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." Fed. R. Civ. P. 26(c)(1). "The burden is upon the party seeking non-disclosure or a protective order to show good cause [and] the trial court has broad discretion to decide when a protective order is appropriate and what degree of protection is required." *Melendez v. Primavera Meats, Inc.*, 270 F.R.D. 143, 144 (E.D.N.Y. 2010) (internal quotations, alterations, and citations omitted). Lastly, under Rule 37, a party may move for an order to compel discovery when it has received no response to its interrogatory or document requests,

provided the movant has in good faith conferred with the opposing party in an attempt to secure the sought responses or documents. *Aetna Life Ins. Co. v. Licht*, 2005 WL 180873, at *1 (S.D.N.Y. Jan. 27, 2005) (citing Fed. R. Civ. P. 37(a)(2)(B)).

"Cases involving trade secrets claims follow the normal procedures set by the Federal Rules; however, courts have universally recognized that defining the scope of discovery in trade secrets cases can be particularly difficult, because there is highly sensitive information and proprietary concerns on both sides." *Uni-Sys., LLC v. U.S. Tennis Ass'n*, 2017 WL 4081904, at *4 (E.D.N.Y. Sept. 13, 2017). Courts often require plaintiffs to identify alleged trade secrets with "reasonable particularity" which requires the plaintiff to provide sufficient information to put the defendant on notice of the nature of the claims alleged and allow the defendant to discern the relevancy of any discovery requests. *Id.* (internal citation omitted). Generic descriptions of categories are insufficient to meet the "reasonable particularity" standard. *Id.* (internal citation omitted). The timing regarding the specificity of discovery in a trade secret case is decided on a case-by-case basis. *Powerweb Energy, Inc. v. Hubbell Lighting, Inc.*, 2012 WL 3113162, at *1 (D. Conn. July 31, 2012).

2. Identification of Trade Secrets

Here, Plaintiff alleges it provided Defendants the expertise, materials, and know-how via a joint-venture and partnership that has now soured. Plaintiff further alleges to have met with Defendants and their employees, created guides, testing protocols, training materials, and cybersecurity mapping. Thus, this is not a case where trade secrets or confidential information was pilfered via unauthorized access or otherwise where Plaintiff may not know what was

taken. Plaintiff admits to having provided Defendants with the confidential information and/or trade secrets currently disputed and has provided Defendants with the requisite particularity to put them on notice of the nature of the claims. In essence, Plaintiff claims to have provided Defendants with the tools and know-how to be able to conduct more robust cybersecurity testing in a way in which it was not doing before their joint venture.

Plaintiff's March 29, 2022 letter to defense counsel with over twenty-five bullets of claims provides sufficient information at the discovery stage for Defendants to determine what Plaintiff views to be its confidential information and/or trade secrets. (ECF No. 87, Ex. J.) For example, Plaintiff states the information includes incident response frameworks, industry and regulation specific penetration tests and vulnerability assessments, remediation plans, market research, and advisory protocols. (*Id.*) In the Court's view, these are not generic descriptions in the context of this case and thus it is unclear what other information Plaintiff could provide that would allow Defendants to search and produce relevant documents. *See generally Bytemark, Inc. v. Xerox Corp.*, 2022 WL 120980 (S.D.N.Y. Jan. 11, 2022). Accordingly, Defendants shall refer to the correspondence between the parties and develop search terms to produce any additional relevant documents. To the extent it is necessary for the parties to further meet and confer, the parties shall do so.

Nonetheless, to the extent Plaintiff can provide greater specificity in its requests it should endeavor to do so, as Plaintiff knows exactly what information it provided to Defendants and when. For example, Plaintiff may request documents related to Defendants' cybersecurity mapping protocol as discussed with Defendant Pecoraro on or around July 18, 2017 and any

subsequent use of the same by Defendants. Of note, Plaintiff need not provide the basis for asserting confidentiality or opine on whether the information is already in the public domain, as those issues are beyond the scope of determining what is relevant and proportional under Rule 26.

3. Discovery Requests

Under Rule 34, a requesting party has an obligation to tailor a document request so that it requests only relevant information but also so that it is proportional to the needs of the case. The document requests at issue are not all so tailored. At the same time, a responding party has an obligation to object with specificity and propose a narrowing of the request for purposes of meeting and conferring about its objection to the request. Defendants did not fully comply with their obligation in this regard. Thus, both parties could have done a better job at complying with Rule 34.

Request 19 is wildly overbroad insofar as it requests "all documents and communications" related to a broad swath of documents for a broad category of services for an unlimited time period. Such a request is presumptively improper. Plaintiff has not adequately explained why this request is proportional to the needs of the case. Thus, Defendants need not respond to this request. Plaintiff admits that Edge's services before the joint-venture included anti-virus, web filtering, email filtering, malware protection systems, network devise and firewalls. These services are all encompassed under the cybersecurity umbrella. Thus, any request should be tailored to request documents that would only include Plaintiff's confidential information and/or trade secrets.

Request 23 is also over broad insofar as it requests "all documents and communications" related to a particular employee's work on all responsibilities in relation to cybersecurity offerings. Thus, Defendants need not respond to this request. Plaintiff is directed to consider whether a job description and samples of the types of documents it requests will be sufficient for the needs of the case. Plaintiff is further directed to narrow its requests to focus on Defendants' use of the specific regulatory/governance training modules, diligence checklist, board-level briefing and other materials that it personally developed in accordance with its Scope of Work description while in partnership with Defendants.

Request 31 seeks information that is not relevant to the allegations in Plaintiff's amended complaint. Under Rule 26, Plaintiff is entitled to discovery regarding any nonprivileged matter that is relevant to its claim or defense and proportional to the needs of the case. Here, Plaintiff only alleges that the GDPR provided a lucrative opportunity for the joint-venture and Defendants were stalling in executing their European agreement to take advantage of the compliance related business the new regulation would provide. Plaintiff does not assert it provided any confidential information or trade secrets specific to the GDPR to the Defendants. Accordingly, Defendants need not respond to this request.

Request 38 is also overbroad insofar as it requests "all Statements of Work" for a seven-year period regardless of whether it included use of materials identical or similar to those she prepared while in partnership with Defendants. It is also duplicative of Request 19. Defendants shall only be required to produce Statements of Work prepared from 2016 to date that incorporated Plaintiff's materials or materials similar thereto. The parties are directed to meet

and confer as to whether samples of Statements of Work for cybersecurity services that do not incorporate Plaintiff's materials or materials similar thereto are relevant.

Request 45 is also overbroad insofar as it requests "All documents" related to advertising, sale, promotion, or marketing of cybersecurity services for a five-year period. Defendants shall produce representative samples for this period.

Requests 48, 49, and 50 seek information about revenues and profits from products wholly unrelated to CyberSAIF. Plaintiff has not adequately explained why these requests are relevant and proportional to the needs of the case. Thus, Defendants need not produce this information. To the extent there are relevant revenue streams that may touch on Plaintiff's claims, Plaintiff shall tailor any requests accordingly.

Lastly, to the extent Defendants have yet to comply with the remaining document requests to which they do not object, they are ordered to do so. Any such objection is deemed waived as untimely. *See Cohalan v. Genie Indus., Inc.*, 276 F.R.D. 161, 163 (S.D.N.Y. 2011).

4. Motion to Seal

The parties' motion to seal is GRANTED. The contemplated document is a business document containing internal strategies and processes that warrants sealing. *See Automated Mgmt. Sys., Inc. v. Rappaport Hertz Cherson Rosenthal, P.C.*, 2022 WL 1450737, at *2 (S.D.N.Y. May 9, 2022) (citing *Whittaker v. MHR Fund Mgmt.* LLC, 2021 WL 4441524, at *2 (S.D.N.Y. Sept. 28, 2021) ("In the context of business documents like those at issue here, a party may overcome the presumption of access upon a showing of higher values such as 'the protection of sensitive, competitive, or proprietary business information.'").

CONCLUSION

For the reasons stated above, Defendants' motion is DENIED (ECF No. 82), Plaintiff's motion is GRANTED in part and DENIED in part (ECF No. 86), and the parties' joint motion to seal at ECF No. 85 is GRANTED. Within two weeks, the parties shall meet and confer to determine a production schedule consistent with this Order.

SO ORDERED.

DATED: New York, New York
June 3, 2022

Katharine H Parker

KATHARINE H. PARKER
United States Magistrate Judge